Ordonnance sur le système de traitement des données relatives à la protection de l'Etat (Ordonnance ISIS)

du 30 novembre 2001 (Etat le 1er janvier 2009)

Le Conseil fédéral suisse,

vu les art. 15, al. 3 et 5, et 30, de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[1],
vu les art. 31*c*, 32*a* et 32*b* de la loi fédérale du 20 juin 1997 sur les armes[2],[3]
arrête:

Section 1 Dispositions générales

Art. 1 Objet

La présente ordonnance règle l'exploitation, le contenu des données et l'utilisation du système de traitement des données relatives à la protection de l'Etat (ISIS).

Art. 2 Buts

1 ISIS a pour but de faciliter:

a. la mise en œuvre de mesures préventives dans le domaine de la protection fédérale de l'Etat;

b. les tâches de police de sécurité et de police administrative;

c. l'exécution de la législation sur les armes;

2 ISIS est utilisé pour:

a.[4] l'exécution de travaux de recherche et d'analyse des données saisies;

b. l'élaboration de rapports de situation;

c. l'exécution de travaux administratifs;

RO **2001** 3173

1 RS **120**
2 RS **514.54**
3 Nouvelle teneur selon le ch. II 1 de l'annexe 4 à l'O du 2 juillet 2008 sur les armes, en vigueur depuis le 12 déc. 2008 (RS **514.541**).
4 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).

d. le classement et la gestion de dossiers;

e.[5] l'exécution de travaux de documentation;

f.[6] la gestion des affaires.

Art. 3[7] Définitions

Dans la présente ordonnance, on entend par:

a. données: informations mémorisées dans ISIS;

b. objets: regroupements de données se rapportant à une ou plusieurs personnes, faits ou événements;

c. communications: nouvelles informations relatives à un ou plusieurs objets;

d. relations: liens entre des objets et des communications spécifiques;

e. blocs de données: communications et relations relatives à un objet;

f. données OCR: données de dossiers saisies de telle manière qu'une recherche dans l'ensemble du texte est possible;

g. données d'image: documents consultés sous forme d'image;

h. consultations ponctuelles: consultations en ligne pour déterminer si une personne figure dans ISIS;

i. tiers: personnes ou organisations revêtant une importance du point de vue de la protection de l'Etat uniquement de par leur lien avec un objet;

j. factsheets: appréciations périodiques standardisées de l'analyse stratégique relative à un objet spécifique.

Art. 4[8] Systèmes et banques de données

[1] ISIS se compose des systèmes et banques de données suivants:

a. «ISIS00 Général» avec classement des dossiers, gestion des mandats, analyse des risques, statistique et module d'archivage;

b.[9] «ISIS01 Protection de l'Etat» avec les banques de données «Protection de l'Etat», «Documentation» et «Système numérique»;

c. «ISIS02 Administration» avec la banque de données «Administration»;

5 Introduite par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
6 Introduite par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
7 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
8 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
9 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).

d.[10] «ISIS03 Armes» avec les banques de données «Acquisition d'armes par des étrangers», «Révocation d'autorisations et mise sous séquestre d'armes» et «Police administrative»;

e. «ISIS04 Explosifs» avec la banque de données «BARBARA»;

f. «ISIS05 News» avec les banques de données «NEWS», «Portail interactif pour Open Sources», «ELIS», «IPIS», «Infopress» et «ISIS-Info»;

g. «ISIS06 Contrôles de sécurité relatifs aux personnes» avec la banque de données «Contrôles de sécurité relatifs aux personnes».

2 Les banques de données contiennent les informations suivantes:

a. «Protection de l'Etat» (ST): informations relatives aux personnes et aux événements, tirées des activités préventives déployées dans le domaine de la protection de l'Etat;

b.[11] «Police administrative» (VP): informations relatives aux personnes et aux événements relevant du domaine des offices centraux de police administrative de l'Office fédéral de la police (fedpol);

c. «Documentation» (DO): informations documentaires relevant de l'ensemble du domaine d'activité du SAP, conformément à l'art. 11 de l'ordonnance du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (OMSI)[12];

d. «Système numérique» (NU): informations relatives aux événements, tirées de programmes déterminés de recherches;

e. «Administration» (VE): informations nécessaires au contrôle des affaires;

f. «Acquisition d'armes par des étrangers» (DEWA): informations personnelles concernant l'acquisition d'armes par des ressortissants étrangers non titulaires d'un permis d'établissement en Suisse;

f[bis].[13] «Acquisition d'armes par des personnes domiciliées dans un autre Etat Schengen» (DEWS): informations personnelles concernant l'acquisition d'armes ou d'éléments essentiels d'armes par des personnes domiciliées dans un autre Etat lié par l'un des accords d'association à Schengen;

g. «Révocation d'autorisations et mise sous séquestre d'armes» (DEBBWA): informations personnelles concernant la révocation d'autorisations et la mise sous séquestre d'armes en Suisse;

10 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
11 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
12 RS **120.2**
13 Introduite par le ch. II 1 de l'annexe 4 à l'O du 2 juillet 2008 sur les armes, en vigueur depuis le 12 déc. 2008 (RS **514.541**).

g^bis.[14] «Remise et retrait d'armes de l'armée» (DAWA): informations relatives aux personnes qui se sont vu remettre une arme en propriété ou qui se sont vu retirer en vertu de la législation militaire leur arme personnelle ou l'arme qui leur avait été remise en prêt;

g^ter.[15] «Exploitation des traces laissées par des armes à feu» (ASWA): informations personnelles destinées à l'exploitation des traces laissées par des armes à feu sur des armes, des munitions, en particulier des munitions utilisées pour la commission de délits, et des personnes impliquées dans des délits ou concernées par des délits.

h. «BARBARA»: informations relatives aux événements, tirées du domaine d'activité de l'Office central pour les explosifs et la pyrotechnie;

i. «NEWS»: communiqués de presse relevant de la protection de l'Etat, tirés d'Internet;

j. «Portail interactif pour Open Sources» (IPOS): portail personnalisé permettant d'utiliser des sources d'information accessibles au public;

k. «ELIS»: représentation électronique de la situation en matière de sécurité intérieure;

l. «IPIS»: communiqués des agences de presse relevant de la protection de l'Etat;

m. «Infopress»: revue de presse quotidienne établie par le SAP;

n. «ISIS-Info»: plate-forme d'information destinée aux utilisateurs d'ISIS;

o. «Contrôles de sécurité relatifs aux personnes» (PSP): informations nécessaires au contrôle des affaires dans le domaine des contrôles de sécurité relatifs aux personnes.

3 Les accords d'association à Schengen sont mentionnés en annexe. [16]

Art. 5[17] Données traitées

1 Les données enregistrées dans les banques de données d'ISIS sont classées en catégories en fonction des domaines spécialisés, dans la mesure où cette classification est judicieuse pour la gestion des accès.

14 Introduite par le ch. II 1 de l'annexe 4 à l'O du 2 juillet 2008 sur les armes, en vigueur depuis le 12 déc. 2008 (RS **514.541**).
15 Introduite par le ch. II 1 de l'annexe 4 à l'O du 2 juillet 2008 sur les armes, en vigueur depuis le 12 déc. 2008 (RS **514.541**).
16 Introduit par le ch. II 1 de l'annexe 4 à l'O du 2 juillet 2008 sur les armes, en vigueur depuis le 12 déc. 2008 (RS **514.541**).
17 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).

2 Les banques de données d'ISIS sont structurées selon les critères ci-après: communications, objets et relations. Les différents champs de données sont réglés par le Département fédéral de la défense, de la protection de la population et des sports (DDPS) et par le Département fédéral de justice et police (DFJP) dans leur domaine de compétence fixé à l'art. 22. [18]

Art. 6 Intranet

1 L'«Intranet ISIS» est un système de communication codé au sein d'ISIS.[19]

2 Le SAP ne met ce système qu'à la disposition des utilisateurs d'ISIS.

Section 2 Utilisateurs, raccordement et accès aux données

Art. 7[20] Utilisateurs

1 Les utilisateurs d'ISIS sont les suivants:

a. les agents du Service d'analyse et de prévention (SAP) et ceux des organes cantonaux chargés du maintien de la sûreté intérieure; ils sont raccordés au système par une procédure d'appel;

b. les collaborateurs du Service fédéral de sécurité (SFS), de la Police judiciaire fédérale (PJF), des offices centraux des armes, pour les explosifs et la pyrotechnie et le service compétent pour décider de mesures d'éloignement à l'encontre d'étrangers conformément aux art. 67, al. 2, et 68 de la loi fédérale du 16 décembre 2005 sur les étrangers[21]; ils peuvent effectuer des consultations ponctuelles par une procédure d'appel;

c. les collaborateurs du Service fédéral chargé des contrôles de sécurité relatifs aux personnes (intégré à la Division de la protection des informations et des objets); ils peuvent effectuer des consultations ponctuelles par une procédure d'appel.[22]

2 Les utilisateurs d'ISIS ont accès aux données nécessaires à l'accomplissement de leurs tâches légales.

3 Les organes cantonaux chargés du maintien de la sûreté intérieure ne peuvent pas consulter les données classifiées issues des contacts directs avec les autorités de sécurité étrangères.

18 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
19 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
20 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
21 RS **142.20**
22 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).

4 Les droits d'accès sont réglés par le DDPS et le DFJP dans leur domaine de compétence fixé à l'art. 22. Le directeur du SAP ou de fedpol, ou leurs suppléants statuent sur les demandes individuelles. [23]

5 La Section Assurance qualité du SAP et l'unité compétente auprès de fedpol sont responsables de l'application des droits d'accès dans leur domaine de compétence fixé à l'art. 22. [24]

Art. 8[25] Raccordement des cantons

Le DDPS[26] fixe les conditions du raccordement des organes cantonaux chargés du maintien de la sûreté intérieure, lesquels ne sont raccordés à ISIS qu'une fois ces conditions remplies.

Art. 9[27]

Section 3 Traitement des données

Art. 10 Saisie des données et contrôle de qualité

1 Seules peuvent être traitées dans ISIS des informations qui répondent aux buts définis à l'art. 2.

2 La Section Analyse préliminaire du SAP introduit les données dans ISIS et détermine la catégorie de communications.[28]

2bis Les personnes suivantes peuvent également introduire des données et déterminer les catégories de communications:

a. les collaborateurs du Service des étrangers du SAP: données issues du contrôle des photos d'identité;

b. les collaborateurs de l'Office central des armes de fedpol: données issues des banques de données DEWA, DEWS, DEBBWA, DAWA et VP;

c. les collaborateurs de l'Office central pour les explosifs et la pyrotechnie de fedpol: données issues des banques de données BARBARA et VP;

d. les collaborateurs de l'Analyse du SAP: factsheets;

23 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
24 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
25 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
26 Nouvelle expression selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
27 Abrogé par le ch. I de l'O du 30 juin 2004, avec effet au 1er sept. 2004 (RO **2004** 3495).
28 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).

e. les collaborateurs du Domaine Contrôles de sécurité relatifs aux personnes: données issues de la banque de données PSP.[29]

3 Les données destinées aux banques ST et VP sont, dans un premier temps, saisies provisoirement (code «p»). Leur fiabilité est appréciée en fonction de la provenance, du mode de transmission, du contenu et des informations déjà disponibles (code «g» pour les communications fiables et code «u» pour celles qui ne le sont pas).[30]

4 La Section Assurance qualité du SAP et l'unité compétente auprès de fedpol vérifient, dans leur domaine de compétence fixé à l'art. 22, les saisies provisoires, notamment l'indication des sources, l'appréciation de la fiabilité et la date de la prochaine appréciation globale; enfin, elle confirme l'enregistrement définitif des données (code «k»). [31]

5 Le directeur du SAP et de fedpol, respectivement leurs suppléants, peuvent charger l'Assurance qualité d'apprécier le contenu des autres banques de données dans leur domaine propre de compétence. [32]

Art. 11[33] Classement des dossiers

1 Le classement des dossiers doit garantir leur gestion et leur archivage conformément aux instructions.

2 Les informations à l'origine des objets et des communications peuvent être saisies comme données OCR, sauf dans les banques de données ST, BARBARA et PSP, où elles sont saisies uniquement comme données d'image.

3 Il est possible de renoncer au classement-papier des dossiers dans la mesure où les informations à l'origine des objets et des communications sont saisies comme données d'image.

Art. 12 Consultation des banques de données

1 Les données peuvent être consultées suivant les critères ci-après: objets, relations, communications, mandats et recherche dans l'ensemble du texte. Les données d'image ne peuvent pas être consultées séparément.[34]

2 La consultation des communications n'est possible que dans un seul système à la fois.[35]

29 Introduit par le ch. I de l'O du 30 juin 2004 (RO **2004** 3495). Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
30 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
31 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
32 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
33 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
34 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
35 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).

3 Les agents du SAP spécialement formés peuvent procéder à des appréciations dans le cadre de leur domaine d'activité.

4 Les objets et leurs relations peuvent être représentés et enregistrés visuellement.[36]

Art. 13 Communication de données

1 Dans des cas déterminés, le SAP peut communiquer des données traitées dans ISIS, à l'exception des données prélevées dans le cadre de contrôles de sécurité relatifs aux personnes: [37]

a. aux autorités pénales cantonales, aux fins de prévenir et de poursuivre les actes punissables;

b. au Département fédéral des affaires étrangères (DFAE), pour l'appréciation des demandes d'accréditation et du droit de séjourner en Suisse de ressortissants d'Etats étrangers ou de membres d'organisations internationales, en vue du respect des engagements de protection découlant du droit international public ainsi que dans le cadre du droit de coopérer du DFAE dans le domaine de la législation régissant les échanges extérieurs;

c. [38] à fedpol:

1. pour soutenir les enquêtes de police judiciaire, ainsi que dans le cadre de recherches préliminaires utiles à l'établissement de faits dans le domaine de la lutte contre le crime organisé et le trafic illicite des stupéfiants,
2. dans le cadre de l'entraide administrative internationale liée à des affaires pénales (INTERPOL),
3. pour saisir des informations dans le système de recherches informatisées de police RIPOL et dans le N-SIS,
4. pour apprécier les risques sur le plan sécuritaire lors de la mise en œuvre de mesures de protection en faveur de personnes ou de bâtiments;

d. à l'Office fédéral de la justice, pour compléter ou exécuter une requête d'entraide judiciaire en matière pénale;

e.[39] à l'Office fédéral des migrations pour l'application de mesures contre des étrangers, notamment en vue de leur éloignement, ainsi que pour traiter des demandes de naturalisation et pour apprécier des demandes d'asile;

f. …[40]

36 Introduit par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
37 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
38 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
39 Nouvelle teneur selon le ch. 2 de l'annexe à l'O du 3 nov. 2004, en vigueur depuis le 1er janv. 2005 (RO **2004** 4813).
40 Abrogée par le ch. 2 de l'annexe à l'O du 3 nov. 2004, avec effet au 1er janv. 2005 (RO **2004** 4813).

g.[41] à d'autres unités administratives du DDPS pour l'exercice du droit de coopérer du DDPS dans le domaine de la législation régissant les échanges extérieurs;

h. au Service de sécurité militaire pour:

1. apprécier la situation militaire en matière de sécurité,
2. protéger des informations et des ouvrages militaires,
3. exécuter, dans le domaine de l'armée, des tâches en matière de police criminelle et de police de sécurité,

et, lorsque les membres du service sont mis sur pied pour un service actif, pour:

4. garantir la sécurité préventive de l'armée à l'égard de l'espionnage, du sabotage et d'autres activités illicites,
5. rechercher des renseignements,
6. veiller à la protection de personnes occupant des postes de représentants de l'Etat;

i.[42] au Service de renseignement stratégique du DDPS, dans le contexte d'informations importantes pour la politique de sécurité, et au Service de renseignement militaire du DDPS, en relation avec des informations qui peuvent avoir une importance pour l'armée;

j. à la justice militaire, pour l'exécution de tâches de police judiciaire et de police de sécurité;

k. aux organes des gardes-frontière et de la douane, pour localiser des personnes, opérer des contrôles douaniers et effectuer des enquêtes pénales administratives;

l. au Secrétariat d'Etat à l'économie, pour l'application de la loi fédérale du 13 décembre 1996 sur le matériel de guerre[43], et pour l'exécution de mesures dans le domaine de la législation régissant les échanges extérieurs;

m. à l'Office fédéral de la formation professionnelle et de la technologie, pour l'octroi de permis d'emploi de substances explosibles;

n. à l'Office fédéral de l'aviation civile et à La Poste Suisse, pour l'exécution des mesures en matière de police de sécurité;

o. à l'Office fédéral de l'énergie, pour l'application de la loi du 23 décembre 1959 sur l'énergie atomique[44] et pour l'exercice de son droit de coopérer dans le domaine de la législation régissant les échanges extérieurs;

41 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
42 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
43 RS **514.51**
44 [RO **1960** 585, **1983** 1886 art. 36 ch. 2, **1987** 544, **1993** 901 annexe ch. 9, **1994** 1933 art. 48 ch. 1, **1995** 4954, **2002** 3673 art. 17 ch. 3, **2004** 3503 annexe ch. 4. RO **2004** 4719 annexe ch. I 1]. Voir actuellement la loi du 21 mars 2003 sur l'énergie nucléaire (RS **732.1**).

p.[45] aux services de la Confédération et des cantons compétents pour initier des contrôles de sécurité relatifs aux personnes (services requérants), au service fédéral chargé de la mise en œuvre de ces contrôles (intégré à la DPIO) ou aux services spécialisés des cantons;

q. aux organes administratifs concernés, pour assurer leur sécurité;

r. à des organes administratifs et à des particuliers, pour leur permettre de motiver une demande de renseignements;

s. à des particuliers, pour écarter un danger considérable;

t.[46] à des autorités de sécurité étrangères, dans le cadre des demandes de clearing (demandes de conformité); les données qui ne sont pas dans l'intérêt de la personne concernée ne peuvent être transmises qu'avec l'accord exprès de celle-ci;

u.[47] à l'Office européen de police (Europol), aux fins de la coopération prévue par l'Accord du 24 septembre 2004 entre la Confédération suisse et l'Office européen de police[48].

2 Pour la communication à l'étranger, sont applicables les art. 17, al. 3 à 5, et 7 LMSI.

3 La communication de données n'est pas autorisée lorsque des intérêts prépondérants publics ou privés s'y opposent.

4 Lors de toute communication, le destinataire doit être renseigné sur la fiabilité et l'actualité des données (art. 10). Il ne peut utiliser les données que dans le but pour lequel elles lui ont été transmises. Il doit être rendu attentif aux restrictions d'emploi et au fait que l'autorité qui communique les données se réserve le droit de se renseigner sur l'utilisation qui en aura été faite.

5 La communication, ainsi que ses destinataires, son objet et ses motifs, doivent être enregistrés.

6 La communication de données issues des banques DEWA, DEWS, DEBBWA, DAWA et ASWA est régie par les art. 63 et 64 de l'ordonnance du 2 juillet 2008 sur les armes[49].[50]

Art. 14 Copie de données

1 Les données d'ISIS ne peuvent être reportées dans d'autres fichiers ni par le biais d'installations de communication ni au moyen de supports de données. L'archivage

45 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
46 Introduite par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
47 Introduite par le ch. I de l'O du 10 mars 2006 (RO **2006** 921).
48 RS **0.360.268.2**
49 RS **514.541**
50 Nouvelle teneur selon le ch. II 1 de l'annexe 4 à l'O du 2 juillet 2008 sur les armes, en vigueur depuis le 12 déc. 2008 (RS **514.541**).

électronique des données d'ISIS aux Archives fédérales n'est pas soumis à la présente disposition.

2 Des données d'ISIS peuvent être passagèrement transférées dans des banques de données de travail aux fins de travaux d'exploitation particuliers. Ceux-ci terminés, les données doivent être effacées.

Art. 15 Droit d'être renseigné

1 Le droit d'être renseigné est régi par l'art. 18 LMSI.

2 Le droit d'être renseigné sur les banques de données DEWA, DEWS, DEBBWA, DAWA et ASWA est régi par l'art. 32*g* de la loi du 20 juin 1997 sur les armes. [51]

Art. 16 Appréciation générale périodique des données de la banque ST

1 La Section Assurance qualité du SAP procède à une appréciation générale de chaque bloc de données au plus tard cinq ans après la saisie de la première communication et trois ans après la dernière appréciation générale.[52]

2 Elle vérifie, à la lumière des dangers et des risques qui menacent la sécurité du pays, si les communications et les objets saisis dans un bloc présentent un degré de vraisemblance élevé s'agissant du risque pour la sécurité intérieure, en vue d'une appréciation administrative, et si les données sont nécessaires pour d'autres tâches de protection de l'Etat.[53]

3 Les communications et les relations qui figurent dans la banque de données depuis plus de trois ans, avec l'appréciation «peu fiables», ne peuvent continuer d'être traitées comme telles (code «u») jusqu'à la prochaine appréciation générale que si elles sont nécessaires à l'accomplissement de tâches légales et si le chef du SAP ou l'un de ses suppléants en a autorisé le traitement.[54]

4 Les objets identifiés depuis plus de trois ans comme des données relatives à des tiers sont effacés lors de l'appréciation générale.[55]

5 L'Assurance qualité efface les données devenues inutiles. En cas de traitement ultérieur de données encore nécessaires, la date de la dernière appréciation générale doit être enregistrée.

51 Nouvelle teneur selon le ch. II 1 de l'annexe 4 à l'O du 2 juillet 2008 sur les armes, en vigueur depuis le 12 déc. 2008 (RS **514.541**).
52 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
53 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
54 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
55 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).

Art. 17 Durée de conservation des données

1 Les données de police préventive peuvent être mémorisées dans ISIS pendant une durée maximum de quinze ans.

2 Pour les données ci-après, la durée de conservation maximale est la suivante:

a. 20 ans pour les données relatives à des programmes de recherches de police préventive en cours;

b. dix ans au plus pour les données relatives à des interdictions d'entrée, à compter de leur expiration;

c. cinq ans pour les données recueillies dans le cadre de procédures de contrôles de sécurité relatifs aux personnes;

d. 30 et 10 ans respectivement pour les données relevant de la correspondance avec des organes administratifs et des particuliers.

3 Les données des banques DO, BARBARA, IPOS, NEWS, IPIS, Infopress et ISIS-Info peuvent être conservées pendant une durée illimitée.[56]

4 La conservation des données dans les banques DEWA, DEWS, DEBBWA, DAWA et ASWA est régie par l'art. 66 de l'ordonnance du 2 juillet 2008 sur les armes[57].[58]

Art. 18 Effacement des données

1 A l'expiration de leur durée de conservation, les données sont effacées dans un délai de trois mois, à moins que le chef du SAP ou l'un de ses suppléants ne décide, à la lumière des dangers et des risques existants, qu'elles sont indispensables à l'accomplissement de tâches légales.[59]

2 Dans les cas visés à l'al. 1, la durée de conservation ultérieure des données s'élève à trois ans. Elle ne peut être prolongée qu'une fois.

3 Tout le bloc de données ainsi que toute factsheet éventuelle sont supprimés avec l'effacement de la dernière communication (y compris les relations, données d'image et mandats correspondants).[60]

4 Les données destinées à être supprimées, à l'exception des informations définies à l'art. 20, al. 2, sont transférées dans le module d'archivage.[61]

56 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
57 RS **514.541**
58 Nouvelle teneur selon le ch. II 1 de l'annexe 4 à l'O du 2 juillet 2008 sur les armes, en vigueur depuis le 12 déc. 2008 (RS **514.541**).
59 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
60 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
61 Introduit par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).

Art. 19[62] Données et dossiers des organes cantonaux chargés de la protection de l'Etat

[1] Les organes cantonaux chargés du maintien de la sécurité intérieure peuvent conserver cinq ans au plus après la première saisie les données et les dossiers établis dans le cadre des tâches de protection de l'Etat qu'ils effectuent pour la Confédération.

[2] A l'expiration de leur durée de conservation, les données doivent être effacées et les dossiers détruits.

Art. 20 Obligation de proposer les documents aux Archives fédérales

[1] Les données et les dossiers devenus inutiles ou destinés à être effacés ou détruits sont proposés aux Archives fédérales aux fins d'archivage.[63]

[2] Les documents classifiés (données et dossiers) émanant des relations avec les autorités de sécurité étrangères et de la recherche opérative ne sont pas proposés aux fins d'archivage, mais conservés en interne d'entente avec les Archives fédérales.[64]

[3] Les données que les Archives fédérales jugent sans valeur archivistique sont effacées du module d'archivage. Les autres dispositions légales en matière de destruction de données sont réservées.[65]

[4] Avant la remise des documents d'un dossier personnel aux Archives fédérales, le SAP introduit dans la banque de données VE la date de livraison, le numéro d'enregistrement, ainsi que les données établissant l'identité de la personne concernée; ces informations sont conservées pendant dix ans, puis effacées.

Section 4 Dispositions relatives à l'organisation

Art. 21 Sécurité des données et journalisation

[1] Pour assurer la sécurité des données, sont applicables l'art. 20 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)[66], l'ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale[67] ainsi que les conditions fixées par le DDPS[68] selon

62 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
63 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
64 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
65 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
66 RS **235.11**
67 RS **172.010.58**
68 Nouvelle expression selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).

l'art. 8 de la présente ordonnance pour le raccordement des organes cantonaux chargés du maintien de la sécurité intérieure.[69]

2 Le SAP précise dans un règlement ISIS les mesures organisationnelles et techniques contre le traitement non autorisé des données et les modalités de la journalisation automatique des données.

3 Les données ISIS ne peuvent être transmises que sous forme chiffrée durant toute l'opération de transmission.

Art. 22 Responsabilités et compétences

1 Le SAP assume la responsabilité d'ISIS pour les systèmes et banques de données suivants: «ISIS00 Général», «ISIS01 Protection de l'Etat», «ISIS02 Administration», «ISIS05 News» et «ISIS06 Contrôles de sécurité relatifs aux personnes». Il en édicte le règlement de traitement. [70]

1bis Fedpol assume la responsabilité d'ISIS pour les systèmes et banques de données suivants: «ISIS03 Armes», DEWA, DEWS, DEBBWA, DAWA, «ISIS04 Explosifs» et BARBARA. Il en édicte le règlement de traitement. [71]

2 Le SAP et fedpol sont chargés de la formation et de l'assistance aux utilisateurs et veillent à la mise en œuvre de leurs règlements de traitement. [72]

3 La responsabilité technique intégrale d'ISIS incombe au DDPS. Le prestataire de services du système d'information veille à l'exploitation, à l'entretien et à la sécurité d'ISIS. Les développements ultérieurs du système d'information ISIS s'effectuent en accord avec les responsables de l'application au sein de fedpol. Les détails de la collaboration sont réglés dans un accord administratif. [73]

4 Les conseillers à la protection des données du SAP et de fedpol peuvent vérifier au cas par cas et dans leur domaine de compétence que le traitement de données dans ISIS est bien conforme aux dispositions relatives à la protection des données. [74]

Art. 23 Financement

1 La Confédération finance le transport des données jusqu'aux centraux de raccordement des cantons.

2 Les cantons prennent en charge:

a. les frais d'acquisition et de maintenance de leurs appareils;

69 Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1er sept. 2004 (RO **2004** 3495).
70 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
71 Introduit par le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
72 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
73 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
74 Nouvelle teneur selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).

b. les frais d'installation et d'exploitation de leur réseau de distribution.

Art. 24 Exigences techniques

1 Le DDPS[75] détermine les exigences techniques auxquelles doivent satisfaire les terminaux des cantons.

2 Les détails sont fixés dans le règlement ISIS.

Section 5 Dispositions finales

Art. 25 Abrogation du droit en vigueur

L'ordonnance du 1er décembre 1999 sur le système de traitement des données relatives à la protection de l'Etat[76] est abrogée.

Art. 26[77]

Art. 27 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er janvier 2002.

75 Nouvelle expression selon le ch. 3 de l'annexe à l'O du 12 déc. 2008, en vigueur depuis le 1er janv. 2009 (RO **2008** 6305).
76 [RO **1999** 3461, **2000** 1227 annexe ch. II 1 2027]
77 Abrogé par le ch. I de l'O du 30 juin 2004, avec effet au 1er sept. 2004 (RO **2004** 3495).

Annexe[78]
(art. 4, al. 3)

Accords d'association à Schengen

Les accords d'association à Schengen comprennent les accords suivants:

a. Accord du 26 octobre 2004 entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[79];

b. Accord du 26 octobre 2004 sous forme d'échange de lettres entre le Conseil de l'Union européenne et la Confédération suisse concernant les Comités qui assistent la Commission européenne dans l'exercice de ses pouvoirs exécutifs[80];

c. Accord du 17 décembre 2004 entre la Confédération suisse, la République d'Islande et le Royaume de Norvège sur la mise en œuvre, l'application et le développement de l'acquis de Schengen et sur les critères et les mécanismes permettant de déterminer l'État responsable de l'examen d'une demande d'asile introduite en Suisse, en Islande ou en Norvège[81];

d. Accord du 28 avril 2005 entre la Confédération suisse et le Royaume de Danemark sur la mise en œuvre, l'application et le développement des parties de l'acquis de Schengen basées sur les dispositions du Titre IV du Traité instituant la Communauté européenne[82];

e. Protocole du 28 février 2008 entre la Confédération suisse, l'Union européenne, la Communauté européenne et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[83].

78 Introduite par le ch. II 1 de l'annexe 4 à l'O du 2 juillet 2008 sur les armes, en vigueur depuis le 12 déc. 2008 (RS **514.541**).
79 RS **0.360.268.1**
80 RS **0.360.268.10**
81 RS **0.360.598.1**
82 RS **0.360.314.1**
83 RS **0.360.514.1**; pas encore publié.